CLAIMS:

1. A security management method for a network system in which a client, an application server and an integrated authentication server can communicate with each other through a network, comprising the steps of:

making a service request by transmitting information of a certificate from said client to said application server;

transmitting the information of the certificate from said application server to said integrated authentication server to request said integrated authentication server to confirm said certificate;

confirming, by said integrated authentication server, said certificate and checking a user for right to access said application server; and

if valid, transmitting a user ID and a password to said application server to perform, by said application server, authentication based on said user ID and said password.

2. A security management method for a network system in which a client, an application server and an integrated authentication server can communicate with each other through a network, comprising the steps of:

making a service request by transmitting information of a certificate from said client to said application server;

confirming, by said application server, said certificate and transmitting the information of said

certificate from said application server to said integrated authentication server to request a user ID and a password;

checking, by said integrated authentication server, a user for right to access said application server and if valid, transmitting said user ID and said password to said application server; and

performing, by said application server, authentication based on said user ID and said password.

3. A security management method according to claim 1, wherein said client records, as access history information, results of security check including a result of the confirmation of said certificate which is executed by said integrated authentication server and said application server between initial log-in to the system and final log-off from the system, a result of checking right to access said application server, a result of authentication of said user ID and said password and a result of checking the right to access data held by said application server, said integrated authentication server records, as access history information, the result of the confirmation of said certificate and the result of the security check including checking the right to access said application server, and access conditions of the user is checked by collating the access history information recorded by said client with the access history information recorded by said integrated authentication server.

4. A security management method according to claim 2, wherein said client records, as access history information, results of security check including a result of the confirmation of said certificate which is executed by said integrated authentication server and said application server between initial log-in to the system and final log-off from the system, a result of checking the right to access said application server, a result of authentication of said user ID and said password, a result of checking right to access data held by said application server, said integrated authentication server records, as access history information, the result of the confirmation of said certificate and the result of the security check including checking right to access said application server, and access conditions of the user is checked by collating the access history information recorded by said client with the access history information recorded by said integrated authentication.

5. A computer program implemented on a storage medium readable by an integrated authentication server in a network system in which a client, an application server and said integrated authentication server can communicate with each other through a network, said program comprising the steps of:

(a) receiving information of a certificate transmitted from said client via said application server, and (b) confirming that said certificate is valid;

(c) checking whether a user of said certificate

has the right to access said application server; and

(d) if the results of checking in (b) and (c) are valid, transmitting a user ID of the user and a password to said application server to cause said application server to authenticate said user.

6. A computer program implemented on a storage medium readable by an integrated authentication server in a network system in which a client, application servers and said integrated authentication server can communicate with each other, said program comprising the steps of:

(a) receiving a user ID and a password transmitted from said client through a first application server;

(b) checking whether a user of said user ID has right to access said first application server;

(c) if a result of checking in (b) is valid, preparing a temporal certificate of said user, and (d) transmitting said certificate to said client through said first application server;

(e) receiving information of said certificate transmitted from said client through a second application server;

(f) confirming that said certificate is valid;

(g) checking whether a user of said certificate has right to access said second application server; and

(h) if results of checking in (f) and (g) are valid, transmitting a user ID of said user and a password to said second application server to cause said second

application server to authenticate said user.

7. A security management method for a network system in which a client, an application server and an integrated authentication server execute communication, comprising the steps of:

transmitting information of an integrated certificate from said client to said integrated authentication server to request said integrated authentication server to authenticate said integrated certificate;

performing, by said integrated authentication server, confirmation of said integrated certificate and process for authenticating a user of said client and in connection with a request made by said client for communicating with an application of said application server or a communication partner, checking by, said integrated authentication server, whether a user has right to access said application or right to communicate with said communication partner;

if the result of checking is valid, transmitting a certificate of said client, said application server or said communication partner to an entity concerned in communication;

ciphering, in said client, a communication message to said application server or said communication partner by using key information which is inherent to said client and which paired with information of said certificate;

confirming, in said application server or said

communication partner, said client on the basis of the information of said certificate and decoding said communication message;

ciphering, in said application server or said communication partner, a communication message to said client by using key information which is inherent to said application server or said communication partner and which paired with the information of said certificate; and

confirming, in said client, said application server or said communication partner on the basis of the information of said certificate and decoding said communication message.

8. A security management method for a network system in which a client, an application server and an integrated authentication server execute communication, comprising the steps of:

receiving, in said application server, a certificate revocation list concerning a service in which said application server participates;

transmitting information of a common integrated certificate which a user has in respect of a plurality of kinds of services from said client to said application server;

transferring the information of said integrated certificate from said application server to said integrated authentication server;

carrying out, in said integrated authentication

server, confirmation of said integrated certificate and checking the user for right to access and if results of the confirmation and the checking are valid, transmitting said certificate of said user concerning the service in which said application server participates from said integrated authentication server to said client and said application server;

comparing, in said application server, said certificate with said certificate revocation list; and

when said certificate is found in said certificate revocation list, rejecting a service request from said user to said application server.

9. A security management method for a network system according to claim 8, wherein said integrated authentication server automatically delivers said certificate revocation list to said application server.

10. A computer program stored on a storage medium readable by an integrated authentication server in a network system in which a client, a server or a communication partner and said integrated authentication server can communicate with each other, said program comprising the steps of:

(a) receiving information of an integrated certificate which is transmitted from said client and is common to a plurality of kinds of services;

(b) confirming that said integrated certificate is valid;

(c) checking whether a user of said integrated

certificate has right to access said application server or said communication partner; and

(d) if results of checking in (b) and (c) are valid, transmitting to said client a certificate of said user concerning the service in which said application server participates.

11. A computer program stored on a storage medium readable by an integrated authentication server in a network system in which clients, application servers or communication partners and said integrated authentication server can communicate with each other, said program comprising the steps of:

(a) transmitting to a client which makes a request for a service a certificate of said service; and

(b) transmitting a certificate revocation list to an application server or a communication partner which requires authentication of said client.

12. A network system comprising:

a client responsive to a service selection from a user to transmit, together with a service request, a common integrated certificate which is defined for individual users in respect of a plurality of kinds of services to an application server through a network;

said application server adapted to receive said service request and said integrated certificate and transfer said integrated certificate to an integrated authentication server through said network; and

said integrated authentication server adapted

to transmit security information of said user, which is necessary for the process of authentication between said client and said application server and which concerns a service in which said application server participates, through said network when said received integrated certificate is confirmed to be valid.

13. A network system comprising:

a client responsive to a service selection from a user to transmit, together with a service request, a common integrated certificate which is defined for individual users in respect of a plurality of kinds of services to an application server through a network;

said application server adapted to receive said service request and said integrated certificate, transfer said integrated certificate to an integrated authentication server through said network and have a certificate revocation list concerning a service in which said application server participates; and

said integrated authentication server adapted to transmit a certificate of said user which concerns the service in which said application server participates and which is necessary for the process of authentication between said client and said application server when said received integrated certificate is confirmed to be valid,

wherein when said certificate is included in said certificate revocation list at time that said application server receives said certificate, together with said service request, from said client, said

application server rejects authentication process mutual with said client.

14. A network system according to claim 12, wherein said integrated authentication server confirms whether said integrated certificate is valid.

15. A network system according to claim 12. wherein said application server confirms whether said integrated certificate is valid.